Scanning im IPv6-Adressraum

Isabell Egloff[2655897]

Hochschule für Angewandte Wissenschaften Hamburg, Germany
Isabell.Egloff@haw-hamburg.de
https://www.haw-hamburg.de

Abstract. Der IPv4-Adressraum lässt sich relativ schnell durchscannen. Daraus ergaben sich bis heute viele wertvolle Forschungsergebnisse. Nach IPv4 kam IPv6 und die Größe des Adressraumes änderte sich dadurch massiv. Der IPv6-Adressraum lässt sich nicht im Ganzen messen. In dieser Arbeit soll der Stand der Forschung bezogen auf das Thema Scanning im IPv6-Adressraum untersucht werden. Es sollen resultierende Probleme festgestellt werden und mögliche Lösungsansätze gefunden werden, wie ein solcher Scan durchgeführt werden könnte. Dazu wird relevante Literatur bezogen, die diese Lösungsansätze aufzeigt. Aus den Ergebnissen lässt sich schließen, dass es Möglichkeiten gibt, spezielle Messungen im IPv6-Adressraum durchzuführen. Diese betreffen strukturelle Eigenschaften, aus denen Klassifizierungen möglich sind. Es können aber auch bestimmte Techniken eingesetzt werden, die speziell für solche Messungen entwickelt und über mehrere Forschungsarbeiten hinweg angepasst wurden. Schließlich lässt sich noch feststellen, dass sich aus den vorgegeben Arbeiten und den daraus entwickelten Techniken viele mögliche neue Forschungsarbeiten ergeben, die auf diesen Ergebnissen aufbauen können.

Keywords: IPv6 · IPv6-Hitlisten · DNS-Techniken · Crowdsourcing · Klassifizierung

1 Einleitung

IPv4 ist für umfassende Scans kein großes Problem. Mit ZMap ist es möglich, den gesamten öffentlichen IPv4-Adressraum in weniger als 45 Minuten durchzuscannen [1]. Dem Scannen im IPv6-Adressraum sind durch die Größe des Adressraumes Grenzen gesetzt. Dadurch lässt dieser sich nicht im Ganzen durchscannen. Im nächsten Schritt soll ein essenzielles Grundwissen über IPv6 und die Adressierungsarchitektur geschaffen werden, damit das Verständnis über den Aufbau der Adressen und den damit erheblich größeren Adressraum verdeutlicht werden kann. Infolgedessen sollen bereits existierende Forschungsarbeiten zu diesem Thema untersucht und erläutert werden.
In dieser Arbeit werden Forschungsfragestellungen zum Thema Scanning im IPv6-Adressraum gesammelt und erläutert. Daraus wird der Stand der Forschung verdeutlicht. Anhand der Forschungsergebnisse lassen sich in späteren Arbeiten eigene Messungen und Untersuchungen durchführen. Es wird angestrebt, Methoden zur Entdeckung und Messung von scanbasierten Angriffen in IPv6 zu

entwickeln. Eine solche bereits entwickelte Lösung für IPv4 ist Spoki. Mit diesem reaktiven Echtzeit-Netzwerk-Telekommunikationsprogramm kann die Analyse des ankommenden Netzverkehrs als auch aktive Messungen unterstützt werden [2].
Im Abschnitt Zwei wird das Problem des zu großen Adressraumes für das Scannen verdeutlicht. Im Abschnitt Drei werden aktuelle Forschungsarbeiten vorgestellt, die sich mit dem Scannen im IPv6-Adressraum auseinandersetzten. Im Abschnitt Vier werden die daraus resultierenden Ergebnisse noch einmal aufgegriffen, um den Zusammenhang des besagten Problems herzustellen. Die Zusammenfassung und ein Ausblick sind in Abschnitt Fünf dargelegt.

2 Problembeschreibung und Hintergründe

In diesem Abschnitt soll das Problem von IPv6 im Gegensatz zu IPv4 mit Bezug zum Scanning verdeutlicht werden. Somit wird in diesem Abschnitt die Adressierungsarchitektur von IPv6 erläutert.

2.1 Die IPv6-Adressierungsarchitektur

Bevor eine Untersuchung des IPv6-Adressraumes stattfinden kann, muss zuerst festgestellt werden, wie eine IPv6-Adresse aufgebaut ist. Im RFC 4291 wird Aufschluss über die Adressierungsarchitektur des IP Version 6-Protokolls gegeben. Von IPv4 zu IPv6 vergrößert sich die Adressgröße von 32 Bit zu 128 Bit [5].
Um im Internet Datenpakte zu übermitteln, werden Informationen für die Versendung in einem Header-Format hinterlegt. Das IPv6-Header-Format wird im RFC8200, wie im folgenden Abbild dargestellt.

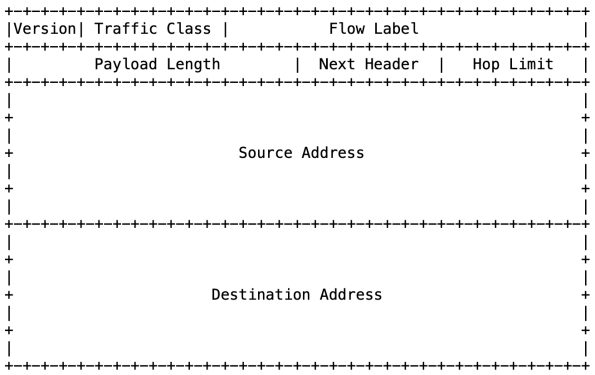

Abbildung 1: IPv6-Header-Format [6]

In diesem Header stehen alle wichtigen Informationen zur Versendung des Datenpaketes. Unter anderem befindet sich hier auch die IPv6-Adresse des Absenders und des Ziels [6]. Eine einzelne IPv6-Adresse, wie sie zum Beispiel in einem solchen Header auftaucht, ist wiederum in Abschnitte unterteilt. Eine solche

Adresse besteht aus einem führenden Netzwerk-Identifikator, der auch (Sub-) Netzwerkpräfix genannt wird. Danach folgt ein Interface-Identifikator (IID). Der Netzwerk-Identifikator wird verwendet, um den für die Adresse bestimmten Datenverkehr zu seinem lokalen Netzwerk zu leiten. Die IID macht die Adresse einer Host-Schnittstelle in einem lokalen Netzwerksegment eindeutig [3].

2.2 Das Problem des IPv6-Adressraumes

Netzwerkmessungen werden benötigt, damit eine verbesserte Verteilung von Inhalten, eine Verkehrsoptimierung, eine Adressanonymisierung oder eine verbesserte Netzwerksicherheit gewährleistet werden kann. Herausforderung ist dennoch der große Adressraum, der nicht vollständig gescannt werden kann. Außerdem sind Subnetzstrukturen unbekannt für die Person, die scannen will [7]. Da das IPv6-Internet um ein Vielfaches größer ist als das, was technisch gesendet oder gespeichert werden kann, ist es nicht machbar, es im Gesamten zu scannen [10]. Dhamdhere et al. stellen fest, dass die Routing-Dynamik in der IPv6-Topologie Ähnlichkeiten zum IPv4-Netz aufzeigt [8]. Bei IPv6 ist außerdem zu erkennen, dass Adresspläne innerhalb von Netzen eine Struktur darstellen. Diese lässt sich für bestimmte Untersuchungen ausnutzen [11].

3 Scanning-Strategien für IPv6

Im Folgenden wird ein Einblick in den aktuellen Forschungsstand von IPv6-Messungen gegeben. Heute bleiben trotz der vielen Untersuchungen noch viele Fragen zu klären. Gerade aus den bisherigen Erkenntnissen können neue Fragestellungen formuliert werden und an den Ergebnissen wird häufig angeknüpft.

3.1 Zeitliche und räumliche Klassifizierung von aktiven IPv6-Adressen

David Plonka und Arthur Berger klassifizieren IPv6-Adressen in die Bereiche "zeitlich" und "räumlich". Die Dimension "zeitlich" bezieht sich dabei auf Zeiträume, in denen eine IPv6-Adresse verwendet wird [3]. Dabei kann es sich um kurze Zeiträume wie ein paar Stunden handeln. Kurze Zeiträume können durch dynamische Adresszuweisungen vorkommen. Bei einer dynamischen Zuweisung weißt ein Dynamic Host Configuration Protocol (DHCP) einem Client eine IP-Adresse für einen begrenzten Zeitraum zu. Das kann nützlich sein, wenn ein Client nur vorübergehend mit dem Netz verbunden ist oder ein Pool von IP-Adressen innerhalb einer Gruppe von Clients geteilt wird, die keine permanenten Adressen benötigen [4].

Es soll bei der zeitlichen Dimension die Lebensdauer der Adressen bestimmt werden können. Wodurch sich beständige oder stabile Adressen von denen trennen lassen, die es nicht sind. Die Adressen werden in Stabilitätsklassen eingeteilt, die nach der Länge des Zeitraums benannt sind, über den die Stabilität bewertet

wurde. Ist eine Adresse über das vergangene Jahr beobachtet worden, wird sie als "1y-stabil (-1y)" eingestuft. Liegt die Dauer der Beobachtung bei 6 Monaten, wird sie in "6m-stabil (-6m)" klassifiziert. Tage werden wiederum mit "d-stable" gekennzeichnet [3].

Tabelle 1: Stabilität von IPv6-Adressen pro Tag [3]

addr class	Mar 17, 2014	Sep 17, 2014	Mar 17, 2015
3d-stable	13.7M (9.22%)	13.6M (6.84%)	30.1M (9.44%)
not 3d-stable	134M (90.8%)	185M (93.2%)	288M (90.6%)
6m-stable (-6m)		588K (.296%)	1.08M (.340%)
1y-stable (-1y)			328K (.103%)

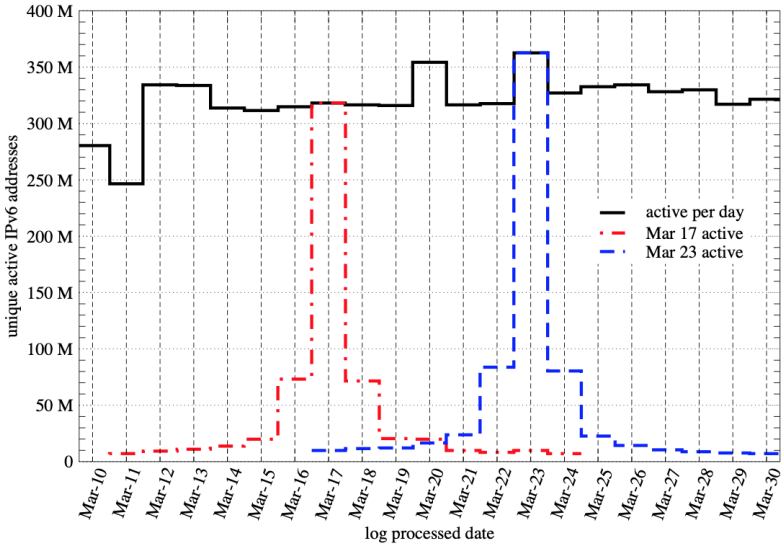

Abbildung 2: IPv6-Adressstabilität [3]

Das Ergebnis der Abbildung 2 zeigt, dass am 17. März 2015 etwa 320 Millionen WWW-Client-IPv6-Adressen beobachtet wurden. Von diesen Adressen sind rund 75 Millionen auch am Tag davor beobachtet worden und rund 20 Millionen am Tag davor. In Tabelle 1 kann festgestellt werden, dass an diesem Tag somit auch 30,1 Millionen 3d-stabile Adressen (9,44 %) aktiv waren. Es wird außerdem eine Messung auf eine Woche erweitert und schließlich festgestellt, dass es relativ gesehen nicht viele sehr langlebige IPv6-Adressen von WWW-Clients gibt. Es werden nur 1,81 Millionen (0,1 %) als "1y-stabil (-1y) eingestuft [3].

Der Bereich "räumlich" bezieht sich auf die mögliche Anzahl der Bereiche (Präfixe) und Positionen (Adressen) im IPv6-Adressraum. Diese Adressen sollen in aktiver Nutzung klassifiziert werden. Bei der räumlichen Untersuchung soll die topologische Nähe der Adressen bewertet werden können. Aus den aktiven WWW-Client-Adressen, die David Plonka und Arthur Berger am 17. März 2015 beobachtet haben, identifizierten sie 128.000 dichte Präfixe und 1,38 Millionen

darin enthaltende WWW-Client-Adressen. Aus diesen Ergebnissen schließen sie, dass es möglich sein sollte, auf ähnlichen Wegen wie schon beim gesamten IPv4-Adressraum diese dichten Regionen des IPv6-Adressraums zu scannen [3].

3.2 Ausnutzen der strukturellen Eigenschaften

Die Struktur von IPv6-Adressierungsschemata werden oft genutzt, um neue Adressen damit zu finden. Ullrich et al. nutzen musterbasiertes Scannen über einen Algorithmus, um damit automatisch Muster in einer Stichprobe von Datensätzen zu erkennen und auf Grundlage der Erkenntnisse Adressen für das Scannen zu generieren. Als Ergebnis wird festgehalten, dass musterbasiertes Scannen bei der richtigen Anwendung sehr sinnvoll sein kann. Die Nutzung des Algorithmus' bietet daher Vorteile wie das Auffinden von mehreren Adressen und Mustern, er ist anpassbar und lässt sich schwer entschärfen [15].

Foremski et al. hingegen stellen Entropy/IP vor. Das ist ein System, das mit Hilfe von maschinellen Lerntechniken die Strukturen von Internetadressen entdeckt. Grundlagen sind dafür Analysen einer Teilmenge von IPv6-Adressen, die als aktiv bekannt sind. Das System kann außerdem diese eigenen Modelle verwenden, um geeignete Adressen für das Scannen zu generieren [16]. Gasser et al. schaffen es sogar in ihrer Arbeit Entropy/IP noch zu erweitern, indem sie IPv6-Adressen zum Sondieren generieren und eine neue Entropie-Cluster-Technik einführen. Dabei werden bei ihrer Methode netzübergreifende Muster gesucht, während die Methode Entropy/IP innerhalb eines Netzes stattfindet. Das entwickelte Entropie-Clustering kann somit Netzwerke finden, die für zufälliges Scannen anfällig sind. Entropy/IP hingegen kann für jedes dieser Netzwerke eine Trefferliste erstellen. Durch die Verwendung unterschiedlicher Techniken lassen sich daher unterschiedliche Untersuchungen anstellen [10].

Eine weitere Methode wird von Murdock et al. vorgestellt, bei der der dichte Adressraum ausgenutzt wird, um dort benachbarte Adressen zu generieren. Solche Sammlungen von IP-Adressen im Adressraum werden auch als "Seeds" bezeichnet. Um diese Gruppe von Adressen zu bestimmen, wird ein Algorithmus benötigt, der sich 6Gen nennt. Dieser Algorithmus unterscheidet sich von der Technik Entropy/IP insofern, dass er nicht Strukturen von Internetadressen erlernt, sondern dichte Regionen ähnlicher Seeds identifiziert, aus denen er Ziel-Adressen generiert. Dafür ermittelt 6Gen zunächst einmal ähnliche Seeds, bevor er sie in dichte Regionen clustert. Um ähnliche Adressen zu gruppieren, wird eine Ähnlichkeitsmetrik definiert [17]. Hierzu wird die Hamming-Distanz [9] verwendet. Dazu wird die Anzahl der Nibble-Positionen gezählt, die sich zwischen zwei Adressen unterscheiden. Nibble entsprechen hierbei 4 Bits. Danach clustert der Algortihmus die Seeds, hierbei führt er ähnliche Cluster nicht zusammen, sondern erlaubt den Seeds zu mehreren Clustern zu gehören und lässt sie unabhängig voneinander wachsen. Später zeigt sich, dass 6Gen die Mehrheit der Seeds zusammen clustert und dabei nur eine kleine Anzahl von Custern bildet, anstatt eine große Anzahl von kleinen Clustern. 6Gen entdeckte am Ende somit 55 Millionen

ansprechbarer Adressen. Bei der Untersuchung wurde jedoch auch eine kleine Anzahl von Netzwerken entdeckt, die IP-Aliasing aufweisen. Es handelt sich daher zum Teil auch um Knoten in Netzwerken, die mehrere Adressen zugewiesen bekommen. Nach Herausfiltern der Aliasing-Adressen war 6Gen jedoch immer noch in der Lage, über eine Millionen neuer Adressen zu finden [17].

3.3 Scannen mit DNS-Techniken

Eine weitere mögliche Technik, die zum Scannen im IPv6-Adressraum untersucht wird, ist die DNS-Technik. In einem Paper von Strowes wird vorgeschlagen, IPv4 Reverse DNS Lookup zu verwenden, um über DNS-Anfragen Namen zu sammeln, die in IPv6-Adressen aufgelöst werden können. Dabei wurden 965 Kilobyte (k) IPv6-Adressen in 5.531 autonomen Systemen (AS) gefunden, von denen 56% ansprechbar waren [13]. Genauso untersuchten Fiebig et al. die Forschung mit der rDNS-Technik und stellten fest, dass sie keine unmittelbaren Herausforderungen für die Verwendung von rDNS als Datenquelle für die Internetmessungen sehen [14]. Gasser et al. griffen das Thema DNS in Verbindung mit Scanning im IPv6-Adressraum wieder auf, indem sie die Reaktionsfähigkeit von IPv6 mit rDNS als Quelle beurteilten und sind zur Bewertung gekommen, dass rDNS IPv6-Adressen wichtig als Ergänzung zu einer Trefferliste sind [10].

3.4 Crowdsourcing-Plattformen

Über Crowdsourcing-Plattformen lassen sich potenzielle Mitarbeiter rekrutieren, die Tools in Netzwerken betreiben, die nicht von den Freiwilligen abgedeckt werden. Über diese Plattformen werden Dritten kleine Geldbeträge für kleine Aufgaben geboten, für die normalerweise keine Fachkenntnisse erfordert werden und innerhalb weniger Minuten erledigt werden können [18]. Gasser et al. überprüfen diese Möglichkeit, um nicht nur eine Vielzahl von IPv6-Adressen zu entdecken, die zu Servern und Routern gehören, sondern um gezielt Client-Adressen zu sammeln. Die Forschungsgruppe stellt dafür Budget und Technik bereit, um an zwei Crowdsourcing-Plattformen zu testen, wie effektiv diese Lösung ist. Sie finden durch ihr Experiment heraus, dass ihre Nutzer einen hohen Anteil an IPv6-Adressen aufweisen (31 % und 20,6 %). Die folgende Tabelle 2 zeigt die Verteilung der Plattformen, die sich durch die Messungen ergeben.

Tabelle 2: Client-Verteilung in der Crowdsourcing-Studie [10]

	IPv4	IPv6	$ASes_4$	$ASes_6$
Mturk	5707	1787	842	73
ProA	1176	245	272	48

Die Menge an IPv6-Adressen ist darauf zurückzuführen, dass die beiden Plattformen gerade in Ländern mit hoher IPv6-Verbreitung genutzt werden (USA, Indien). Nachdem vom Nutzer die Ergebnisse übersendet wurden, wird jeder IPv6-Adresse alle fünf Minuten eine Echo-Anfrage und eine Traceroute geschickt. Dabei finden sie heraus, dass nur 17,3 % auf mindestens eine Echo-Anfrage reagieren. Nach eigener Testung kann das Problem durch zyklische Adresserweiterungen, Benutzer, die sich abmelden, lokale Firewalls und Filterungen durch Internetanbieter verursacht werden, wodurch sich die Antwortrate somit drastisch verringert. Doch für genauere Ergebnisse sind dafür noch mehr Messungen notwendig. Im Endergebnis halten sie fest, dass Crowdsourcing durchaus zusätzliche Adressen liefert und somit auch als Methode genutzt werden kann. Nichtsdestotrotz sind mehr Forschungsarbeiten notwendig, um signifikante Daten festzuhalten. Messungen müssen schließlich schnell nach der Adresssammlung durchgeführt werden, da die Anzahl der ansprechbaren Clients rapide sinkt [10]. Außerdem lohnt sich für viele Nutzer aus Industriestaaten der Aufwand für solche kleinen Geldbeträge nicht, weshalb es zu einer ungleichmäßigen Verteilung im Ergebnis kommt. Das Verfahren ist somit nicht repräsentativ.

3.5 Scanning mit Hilfe von IPv6-Hitlisten

Zur Vereinfachung des Scannens des IPv6-Adressraumes wird auf Methoden zurückgegriffen, die in der Anfangszeit des IPv4-Internetscannings verwendet wurden. Dabei wurden Listen von Ziel-IP-Adressen verwendet, diese werden auch als Hitlisten bezeichnet. Sie dienen als Teilmenge des zu scannenden Adressraumes. Es handelt sich dabei also nicht um eine Liste mit Namen von Web-Servern. Diese Trefferlisten bestehen aus einer Vielzahl von Quellen in Form von IPv6-Adressen, die ausschließlich aus öffentlich zugänglichen Quellen stammen, um die Forschungsarbeit reproduzierbar zu machen. Dabei ist gar nicht unbedingt die Menge an IP-Adressen in dieser Liste entscheidend, da diese möglicherweise nur für kurze Zeiträume verwendet werden. Eine Herausforderung liegt hierbei somit in der Ansprechbarkeit und der Balance von autonomen Systemen und Präfixen. Gasser et al. bauen auf bereits bekannten Ansätzen von solchen Listen auf. Ihre Forschung basiert auf Methoden vorheriger Forschungsarbeiten, aus denen sie sich eine große IPv6-Hitliste, die mehr als 50 Millionen Adressen enthält, erstellten. Viele dieser Methoden wurden in dieser Arbeit bereits aufgegriffen. Die Hitlisten werden weiter aktualisiert, sodass zukünftig Forschungen damit betrieben werden können [10]. Es werden wöchentlich IPv6-Adress-Listen erstellt. Die steigende Anzahl der gesammelten IPv6-Adressen werden in der folgenden Grafik dargestellt [12].

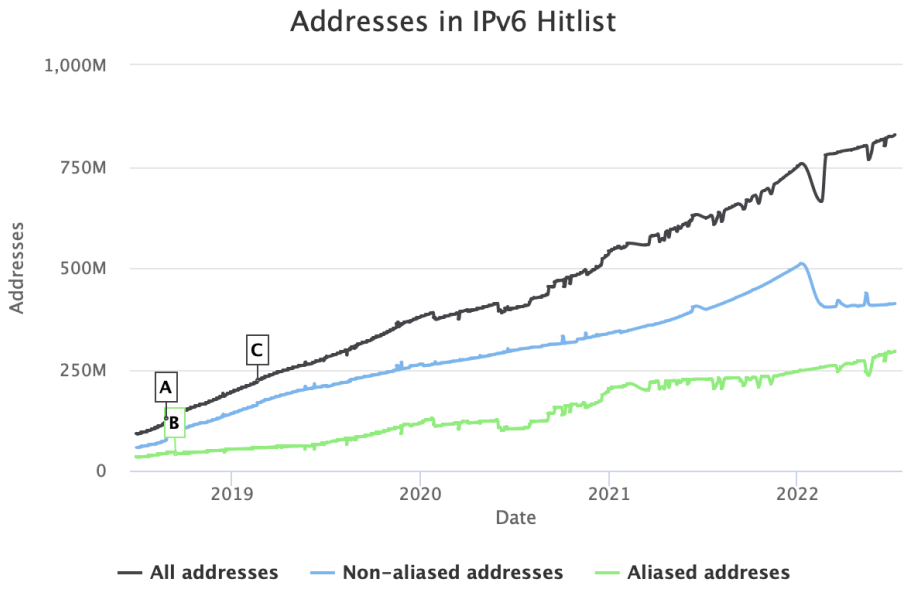

Abbildung 3: Adressen in der IPv6-Hitliste [12]

3.6 Klassifizierung von IPv6-IPv4-Geschwistern

Scheitle et al. identifizieren und klassifizieren verwandte IPv6- und IPv4-Adressen. So eine Zuordnung lässt sich über DNS-Abfragen herausfinden. Daraus ergeben sich IPv6-IPv4-Adresspaare, die denselben Dienst anbieten, aber möglicherweise auf verschiedenen Rechnern gehostet werden. Eine solche Beziehung nennen sie auch "Geschwister". Bei dieser Forschung werden aktive Messungen von TCP-Zeitstempeln und anderen Netzwerkeigenschaften durchgeführt, die anhand von 682 Hosts gemessen werden. Es wird eine Vielzahl von Merkmalen identifiziert und untersucht. Dazu gehört das Fingerprinting mithilfe der TCP Timestamp-Option [19]. Diese Technik wird aus einer vorherigen Arbeit von Beverly und Berger abgeleitet [20]. Netzwork Fingerprinting wird zur Identifizierung von Geräten genutzt. Mit diesen Merkmalen wird ein maschinell erstellter Entscheidungsbaum (ML1) und ein selbst entwickelter Algorithmus (HT) trainiert [19]. Die Lösung scheint nicht wirklich förderlich zu sein, da für ein Fingerprinting die Identifizierung eines Gerätes bereits erfolgt sein muss. Es löst somit nicht das Problem des Auffindens, wie es zum Beispiel bei der rDNS-Technik der Fall ist.

4 Diskussion

In diesem Abschnitt wird noch einmal verdeutlich, welche Ergebnisse aus den verschiedenen Arbeiten gewonnen werden können, um das Problem des Scannens im IPv6-Adressräumen zu umgehen.

Aus den Ergebnissen lässt sich schließen, dass es zu Beginn der Forschung sinnvoll ist festzulegen, welcher Bereich oder welche Eigenschaften von Adressen untersucht werden sollen. Aus dieser Planung lassen sich dann aus vorherigen Forschungsarbeiten Ideen und Vorgänge erschließen. Es muss außerdem geplant werden, inwieweit mit Problemen und Fehlern aus diesen Messungen umgangen werden kann. Genauso gehen auch Gasser et al. in ihrer Arbeit vor. Sie spezialisieren und verändern Messtechniken aus vorherigen Arbeiten, sodass ihre eigene Forschungsarbeit daraus neue Ergebnisse und Entwicklungen entstehen lässt. Durch die Weiterentwicklung und Anpassung von Technologien aus anderen Forschungsarbeiten können neue Ergebnisse gewonnen werden.

Ableitend aus den gesammelten Ergebnissen können strukturelle Eigenschaften und DNS-Techniken genutzt werden, um repräsentative Scan-Ergebnisse zu erzielen. Genauso wird festgestellt, dass bereits erfolgreiche IPv4-Scanning-Techniken auf IPv6-Scans erweitert werden können, um somit bestimmte Bereiche des IPv6-Adressraumes zu scannen.

5 Zusammenfassung und Ausblick

Schlussfolgernd aus den Ergebnissen lässt sich noch einmal zusammenfassen, dass es schon einige Forschungsansätze im Bereich Scanning im IPv6-Adressraum gibt und es sinnvoll ist, auf diesen aufzubauen. Demnach gibt es auch noch viele mögliche Forschungstheorien und -techniken, die weiter entwickelt werden können, um noch bessere Ergebnisse zu erzielen. Das Problem des großen Adressraumes kann somit umgangen werden, indem erst einmal eine bestimmte Art von Adressen untersucht wird. Diese Art lässt sich durch strukturelle Eigenschaften eingrenzen. Entsprechende Algorithmen oder andere selbst entwickelte Lösungen können dabei Abhilfe schaffen. Aus diesen Erkenntnissen können für zukünftige Arbeiten Zusammenhänge, erste Eindrücke und Ideen zum Thema Scanning im IPv6-Adressraum gewonnen werden. Das angestrebte Ziel beinhaltet die Erforschung von Methoden zur Entdeckung und Messung von scanbasierten Angriffen in IPv6.

References

1. Z. Durumeric, E. Wustrow, and J. Halderman. Aug 2013. ZMap: Fast Internet-Wide Scanning and its Security Applica- tions. In Proc. of USENIX Security Symposium, pages 605–620. USENIX.
2. R. Hiesgen, M. Nawrocki, A. King, A. Dainotti, T. C. Schmidt, M. Wählisch. Aug 2022. Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope. 31st USENIX Security Symposium (USENIX Security 22). https://www.usenix.org/conference/usenixsecurity22/presentation/hiesgen.
3. D. Plonka and A. Berger. 2015. Temporal and Spatial Classification of Active IPv6 Addresses. In Proceedings of the 2015 Internet Measurement Conference (IMC '15). Association for Computing Machinery, New York, NY, USA, 509–522. https://doi.org/10.1145/2815675.2815678.

4. R. Droms. March 1997. Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131. https://www.rfc-editor.org/info/rfc2131.
5. R. Hinden and S. Deering. February 2006. IP Version 6 Addressing Architecture. RFC 4291. DOI 10.17487/RFC4291 https://www.rfc-editor.org/info/rfc4291.
6. S. Deering and R. Hinden. July 2017. Internet Protocol, Version 6 (IPv6) Specification. STD 86. RFC 8200. DOI 10.17487/RFC8200. https://www.rfc-editor.org/info/rfc8200.
7. R. Beverly, R. Durairajan, D. Plonka, and J. P. Rohrer. 2018. In the IP of the Beholder: Strategies for Active IPv6 Topology Discovery. In Proceedings of the Internet Measurement Conference 2018 (IMC '18). Association for Computing Machinery, New York, NY, USA, 308–321. DOI 10.1145/3278532.3278559.
8. A. Dhamdhere, M. Luckie, B. Huffaker, k. claffy, A. Elmokashfi, and E. Aben. 2012. Measuring the deployment of IPv6: topology, routing and performance. In Proceedings of the 2012 Internet Measurement Conference (IMC '12). Association for Computing Machinery, New York, NY, USA, 537–550. https://doi.org/10.1145/2398776.2398832.
9. R. W. Hamming. 1950. Error Detecting and Error Correcting Codes. Bell Labs Technical Journal.
10. O. Gasser, Q. Scheitle, P. Foremski, Q. Lone, M. Korczyński, S. Strowes, L. Hendriks and G. Carle. 2018. Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists. IMC '18: Proceedings of the Internet Measurement Conference 2018. 364-378. DOI 10.1145/3278532.3278564.
11. D. Plonka and A. W. Berger. kIP: a Measured Approach to IPv6 Address Anonymization. http://arxiv.org/abs/1707.03900, 2017.
12. https://ipv6hitlist.github.io
13. S. D. Strowes. 2017. Bootstrapping Active IPv6 Measurement with IPv4 and Public DNS. ArXiv abs/1710.08536: n. pag.
14. T. Fiebig, K. Borgolte, S. Hao, C. Kruegel, G. Vigna and A. Feldmann. 2018. In rDNS We Trust: Revisiting a Common Data-Source's Reliability. DOI 10.1007/978-3-319-76481-8_10.
15. J. Ullrich, P. Kieseberg, K. Krombholz and E. Weippl. On Reconnaissance with IPv6: A Pattern-Based Scanning Approach. 2015. 10th International Conference on Availability, Reliability and Security, 2015, pp. 186-192, DOI 10.1109/ARES.2015.48.
16. P. Foremski, D. Plonka, and A. Berger. 2016. Entropy/IP: Uncovering Structure in IPv6 Addresses. In Proceedings of the 2016 Internet Measurement Conference (IMC '16). Association for Computing Machinery, New York, NY, USA, 167–181. DOI 10.1145/2987443.2987445.
17. A. Murdock, F. Li, P. Bramsen, Z. Durumeric and V. Paxson. 2017. Target generation for internet-wide IPv6 scanning. In Proceedings of the 2017 Internet Measurement Conference (IMC '17). Association for Computing Machinery. New York. NY. USA. 242–253. DOI 10.1145/3131365.3131405.
18. Q. Lone, M. Luckie, M. Korczyński, H. Asghari, M. Javed and M. van Eeten. 2018. Using Crowdsourcing Marketplaces for Network Measurements: The Case of Spoofer. Network Traffic Measurement and Analysis Conference (TMA). 2018, pp. 1-8. DOI 10.23919/TMA.2018.8506499.
19. Q. Scheitle, O. Gasser, M. Rouhi and G. Carle. 2017. Large-scale classification of IPv6-IPv4 siblings with variable clock skew. Network Traffic Measurement and Analysis Conference (TMA). pp. 1-9, DOI 10.23919/TMA.2017.8002901.
20. R. Beverly and A. Berger. 2015. Server Siblings: Identifying Shared IPv4/IPv6 Infrastructure Via Active Fingerprinting. 8995. 149-161. DOI 10.1007/978-3-319-15509-8_12.